Guarding Against the Erosion of Competitive Advantage: A Knowledge Leakage Mitigation Model

Research-in-Progress

Atif Ahmad
Department of Computing & Information Systems
University of Melbourne
Parkville, Victoria, Australia
atif@unimelb.edu.au

Heidi Tscherning
Department of Information Systems & Business Analytics
Deakin University
Burwood, Victoria, Australia
heidi.tscherning@deakin.edu.au

Rachelle Bosua
Department of Computing & Information Systems
University of Melbourne
Parkville, Victoria, Australia
rachelle.bosua@unimelb.edu.au

Rens Scheepers
Department of Information Systems & Business Analytics
Deakin University
Burwood, Victoria, Australia
rens.scheepers@deakin.edu.au

Abstract

A critical objective of knowledge-intensive organizations is to prevent erosion of their competitive knowledge base through leakage. Our review of the literature highlights the need for a more refined conceptualization of perceived leakage risk. We propose a Knowledge Leakage Mitigation (KLM) model to explain the incongruity between perceived high-risk of leakage and lack of protective actions. We argue that an organization's perceived risk of leakage increases if competitors can benefit from leakage incidents. Further, perceived leakage risk decreases if the organization is shielded from impact due to their diversity of knowledge assets and their ability to reconfigure knowledge resources to refresh their competitive knowledge base. We describe our approach to the design of a large-scale survey instrument that has been tested and refined in two stakeholder communities: 1) knowledge managers responsible for organizational strategy, and 2) Information security management consultants.

Keywords: Information security/privacy, IS security, Knowledge management capability, Resource-based Theory, Security risk management, Knowledge leakage.

Introduction

The leakage of sensitive organizational data, information and knowledge has become a significant problem in an increasingly networked and global society (DeSouza 2006; Easterby-Smith et al. 2008; Trkman and Desouza 2012), where information and communication technologies, such as social media, cloud computing, and open collaboration technologies challenge the security of organizational boundaries. Leakage occurs when sensitive organizational details, such as intellectual property (IP) and

trade secrets, business strategies, product- or service-related knowledge, or confidential client information, are disclosed (deliberately or inadvertently) to unauthorized entities.

The impact of leakage can be devastating for an organization. Depending on the sensitivity of a leak, the impact may include reputational damage, loss of revenue, and additional costs arising from breaches of confidentiality agreements. In cases where an organization has gained a competitive advantage based on key knowledge (Barney 1991, 1996; Grant 1996, 1997; Mahoney and Pandian 1992), leakage might significantly erode such an advantage (Teece 2007).

The security of an organization's data and information assets is a long-standing area of research in the field of information systems (IS). An extensive body of literature has studied several formal approaches, industry standards, and various security mechanisms to secure an organization's data and information assets (as outlined in the literature review below).

However, when it comes to securing an organization's competitive knowledge, the situation is more complex as knowledge is typically embodied in individuals (e.g., tacit knowledge) or codified in documents and other physical artefacts (e.g., product designs and business processes). Indeed, many of the tried and trusted approaches towards securing organizational data and information assets fail to address the problem of knowledge "walking out the door" (Shedden et al. 2011). As such, it is necessary to have a more encompassing conceptualization of leakage, and leakage mitigation in the case of competitive organizational knowledge.

Considering how reports of knowledge leaks abound in the media, knowledge leakage poses a significant threat to organizations. For example, in October 2013, two scientists at the pharmaceutical corporation Eli Lilly leaked proprietary development on diabetes, cardiology and cancer medication to rival firm Jiangsu Hengrui Medicine. This resulted in the loss of ten years of research believed by Eli Lilley to be worth $55 million (BioSpectrum 2013). In March 2010, Dupont alleged that 149 trade secrets related to its bullet-resistant fabric technology (Kevlar) had been used by its competitor Kolon Industries to develop a rival product (Heracron) (BusinessWeek 2011).

In this study on knowledge leakage, we draw on the definition of Davenport and Prusak (1998) of knowledge as a fluid mix of framed experiences, values, contextual information and expert insight. Our specific focus in this research is on knowledge leakage that occurs through the use of boundary-spanning information and communication technologies. These include leakage through social media (Athanasopoulos et al. 2008; Colwill 2009; Gross and Acquisti 2005; Jagatic et al. 2007), publications (Jansen 2010), email (Carvalho et al. 2009), cloud computing (Ristenpart et al. 2009), and portable data devices (CISCO 2008; Colwill 2009).

Some knowledge leakage may be foreseen by organizations, e.g. when an employee with sensitive knowledge is hired by a competitor (Norman 2001). However, other incidents may occur intentionally but discreetly, e.g. when a competitor draws inferences from various social networking contacts, posts and email conversations (e.g. Furnell and Botha 2011). More often, leakage is accidental, as in the case of offshoring and outsourcing of operations, where sensitive data, information, and knowledge are disclosed to unauthorized parties by mistake (Norman 2001).

This article addresses the fundamental research question: ***how can organizations guard against the leakage of their competitively valuable knowledge?*** In this regard, we focus on organizations with competitively valuable knowledge, which, if leaked, could erode the organization's competitive advantage.

The paper is structured as follows: we review various discipline-specific literatures related to knowledge leakage and protection mechanisms. In particular, we review the literature in organizational strategy, knowledge management, information security management and other related areas. Based on the review, we identify four key unresolved issues related to knowledge leakage. We then revisit our research question and provide a theoretical justification for the research. Subsequently, we synthesize a knowledge leakage mitigation model that frames an organization's capability to guard itself against knowledge leakage, given their perceived leakage risk. We propose that leakage risk is a formative construct comprising of: (1) competitors' capability to benefit from organizational leakage incidents, (2) the organization's knowledge diversification, and (3) the organization's ability to reconfigure its knowledge resources to refresh their competitive knowledge base.

We suggest the inclusion of a competitor perspective and knowledge diversification/reconfiguration constructs in the model to address the unresolved issues we identified in the literature. We conclude with our research approach and key anticipated contributions.

Literature Review

There is a rich discourse in the literature about the differences between data, information and knowledge. Readers are referred to the useful summaries of the key distinctions in sources such as Boisot and Canals (2004) and Dahlbom and Mathiassen (1993). Drawing on the cryptography analogy of Boisot and Canals, raw data becomes information when individuals are able to infer meaning from such data, based on a prior contextual understanding of the background to the data. Furthermore, the literature on intelligence gathering suggests that much knowledge can be inferred from even minimal leakage.

The leakage of data, information or knowledge is therefore to some extent intertwined, as any such leakage could potentially have a detrimental impact on an organization's competitiveness. In this paper, we suggest "knowledge leakage" occurs when an external agency (e.g., a competitor) can infer meaning from divulged data, information or knowledge (based on their understanding of its context), and subsequently leverage such meaning to advance their own competitiveness.

The sections below summarize various bodies of literature that relate to knowledge leakage.

Leakage Mitigation in the Organizational Strategy Literature

The resource-based theory (RBT) (e.g. Barney 1991; Lavie 2006; Leonard-Barton 1992; Penrose 1959; Wernerfelt 1984) is a well-established body of literature that explains how organizations, through their ability to deploy tangible or intangible resources at their disposal effectively, may gain and sustain competitive advantages. RBT suggests that organizational resources and capabilities (in particular if valuable, rare, inimitable, and non-substitutable) deployed in the form of product and services are instrumental to sustaining a competitive advantage (Barney 1996; Barney and Hesterly 2006). This implies that not all organizational knowledge leakage is necessarily competitive advantage-eroding. Clearly, competitive-advantage related knowledge should be the priority in terms of leakage mitigation.

RBT encompasses both tangible and intangible organizational resources (e.g., competitive knowledge) as sources of competitive advantage (Brown and Duguid 2001; Grant 1996; Straub et al. 2004; Teece 2009). The related body of research on dynamic capabilities specifically considers that the protection and reconfiguration of organizational resources and capabilities is a key dynamic capability (Teece 2009). According to this literature, organizations should invest in co-specialized dynamic capabilities to mitigate the erosion of competitive advantages once achieved. In this manner, organizations can then reconfigure their existing resources and capabilities in response to competitors' imitation efforts, to retain competitive advantages. While situating protection of organizational knowledge in the context of deferring competitive advantage erosion, the RBT literature does not offer much advice in terms of specific operational approaches and mechanisms in this regard. These are left to other related literatures as outlined below.

Leakage Mitigation in the Knowledge Management Literature

The knowledge management (KM) literature also views knowledge as a competitive resource in organizations (Davenport and Prusak 1998; Earl 2001; Grant 1996, 1997). The KM literature offers three views that justify the protection of knowledge from leakage. One view explores how to improve knowledge sharing between individuals and groups within the organization (Hansen et al. 1999; Marabelli and Newell 2012; Nonaka 1994), as the increasing flow of knowledge in organizations can drive innovation and productivity (Grant 1997; Nonaka 1994; Nonaka et al. 2000). However, increasing the flow of knowledge also increases the risk of leakage (Holsapple and Jones 2005; Jones and Ashenden 2005; Tan et al. 2010; Trkman and Desouza,2012). The balance between preserving confidentiality and sharing knowledge remains a key dilemma for organizations (DeSouza 2006; Gold et al. 2001; Holsapple and Jones 2005).

The KM literature sources suggest a second view: that in order to maintain a unique and competitive edge, organizations need to invest in knowledge assets that set the organization in a category superior to other competing organizations (Van den Bosch et al. 1999; Volberda et al. 1996). Volatile business environments often force organizations to rapidly change and reconfigure existing knowledge to take the next step towards competitive advantage. To achieve this, a balanced portfolio of diverse knowledge skills and experiences spread across a variety of products and services is required. Such investments save organizations the time to develop existing knowledge and know-how. In addition, diverse knowledge skill sets and experiences facilitate new knowledge creation and the innovative capability of organizations (Smith et al. 2005).

Thirdly, the KM literature sources often distinguish between tacit and explicit knowledge (e.g., Nonaka 1994; Polanyi 1966). Tacit knowledge is inherent and difficult to articulate or codify (Hildreth and Kimble 2002; Polanyi 1966), and is therefore, "sticky" (Szulanski 2000), and to some extent self-protecting, in contrast to codified knowledge (Gold et al. 2001; Teece 2009). Clearly, the leakage of sensitive codified knowledge is of concern to organizations. However, the risk of tacit knowledge leakage arguably increases when an external party is highly knowledgeable. Consider a discussion between two specialists in the same knowledge domain; their shared contextual background might enable them to draw valuable inferences - tacit insights - from each other. By factoring in the capabilities of an external party, it raises the question whether even tacit knowledge is necessarily self-protecting.

Leakage Mitigation in the Information Security Management Literature

Leakage mitigation in the information security management (ISM) literature concerns the preservation of information from disclosure. The majority of the ISM literature focuses on *data* and *information* as opposed to *knowledge*. In terms of the leakage of data and information, there has been considerable research in the computing domain towards developing new approaches to mitigate against potential leakage (see a review of computing approaches in Huth (2013)). Data Leakage Prevention (DLP) systems can be used to analyze, monitor and control the unauthorized transmission of sensitive data (Blasco and Jorge 2013).

Relating to the protection of knowledge, the information security management literature offers two insights:

First, leakage can be mitigated by compartmentalizing information resources according to increasing levels of sensitivity (e.g. 'public', 'restricted'), which relate to secure handling and sharing protocols (Ahmad et al. 2014b; Whitman and Mattord 2011). There is a considerable body of research on technical controls that can be used to enforce and support compartmentalization, such as firewalls and VPNs in the context of networks and biometric devices, user authentication, and role based access control (RBAC) in the context of computing systems (e.g. Liu and Ormaner 2009). The ISM literature also addresses legal mechanisms, such as patents, copyright and the use of non-disclosure agreements (NDAs). These mechanisms are pertinent in collaborations, such as partnership agreements, joint product development, out- and off-shoring (Norman 2001). However, not all intellectual assets can be protected through legal mechanisms, and those that can are not offered long-term protection (Norman 2001).

Second, a renewed focus on the management dimension of information security has led to considerable research on a range of strategies, processes, controls and mechanisms of the managerial, technical, and legal kind that can be used for leakage mitigation purposes (Dhillon 2006; Von Solms 2006). For example, at the managerial level there are risk, policy, and governance related methods, structures and processes that identify what information resources require protection and how that protection can be implemented. Also, an information security culture appears instrumental towards fewer leakage incidents (Siponen 2000; Wilson and Hash 2003).

Other Related Literature

There have been a number of studies focusing on the storage and management of information in organizations. A review of this literature shows the most relevant studies take a risk management approach to examine how organizations handle and store information as part of their routine business processes (e.g. see Shedden et al. 2010; 2011). The literature argues there are three key deficiencies in best-practice Information Security Risk Assessment (ISRA) methods: (1) inability to recognize knowledge

assets; (2) lack of coverage in asset identification (especially assets generated from informal business practices in social environments); and (3) inappropriate level of granularity in the asset identification. The traditional view of ISRAs is that data and information are considered static "assets" that can be enumerated for security accounting and auditing purposes. This view ignores key distinctions between formal and informal handling of information assets and between technology and human involvement in information processes.

The field of intelligence gathering offers a country-level perspective explaining how national intelligence agencies around the world address leakage issues. Similar to the findings in the ISM literature, national intelligence agencies apply security compartments according to the so-called *need-to-know* principle (Michal 1994) using hierarchical categories of classification defined by employee security clearance levels. Despite similarities between the ISM and intelligence literatures, their perspective on leakage risk is entirely different. A key assumption of the intelligence field is that the prevailing environment is fundamentally adversarial and that rival countries will use whatever means possible to acquire as much sensitive information as possible and use it to their best advantage. The risk of leakage is therefore, considered in the context of the *capabilities of external parties*, e.g., rival agencies or known attackers (Jelen 1991; Joint Publication 3-13.3).

Unresolved Issues Relating to Knowledge Leakage

Considering the different perspectives on knowledge leakage, the following are unresolved issues in the literatures related to our fundamental research question:

1. To what extent are the identified approaches, mechanisms and principles articulated in these bodies of literature, and especially the information security literature, applicable to the protection of *knowledge,* as opposed to the protection of data and information for which they were devised?
2. How can we conceptualize an organization's capability to guard its competitive knowledge? How can we determine its adequacy and the protective actions afforded by such a capability? At present there is no comprehensive approach or best-practice standards in this area.
3. How should the risk of knowledge leakage be considered? The intelligence literature suggests that this risk relates to the external parties' intent and capabilities to acquire and exploit such knowledge.
4. Last, how do we understand the relationship between perceived risk and organizational responses to such perceived risks? For example, a recent study (Ahmad et al. 2014a) found no formal and systemized approach to leakage mitigation despite the fact that the organizations were knowledge-intensive, highly competitive and were operating within a turbulent environment (and therefore could be expected to have a perceived high risk of leakage).

The Knowledge Leakage Mitigation (KLM) Model

We propose a research model (see Figure 1) to help address the issues highlighted above, which we have argued are not adequately addressed in the present literature. The theoretical justification for this research stems from RBT, which positions organizational knowledge as a competitive resource that could potentially account for an organization's competitive advantage. We argue that the theoretical justification for this research is the need for a competitive perspective on knowledge protection to be added to RBT.

In conceptualizing the actions an organization might take to protect its knowledge, we also draw on security risk theory. We begin our conceptual development of the model by drawing guidance about leakage mitigation from security risk theory as it underpins all security management activities (Whitman and Mattord 2011). At the most fundamental level, this theory argues that an organization's protective actions must be guided by its security risk exposure. In the context of this project, security risk theory suggests that the higher and organization's (perceived) risk of leakage, the greater the need for protective actions to mitigate that risk.

In this regard our literature review highlights the need for a more refined conceptualization of perceived leakage risk. For example, Ahmad et al. (2014a) examined the knowledge security strategy of eleven knowledge-intensive organizations. They concluded that although the organizations were acutely aware of the security risk to their knowledge assets, they did not have a deliberate strategy to mitigate leakage in

place (i.e., many adopted a 'laissez faire' approach despite being aware of their risk). At face value, this observation conflicts with the fundamental assertion of security risk theory, suggesting there are additional factors at play. Therefore, we draw two key implications for our research study: (1) the relationship between perceived leakage risk and protective actions must be tested with a much larger sample set, and (2) there are additional factors that explain why organizations are not taking protective action against possible leakage.

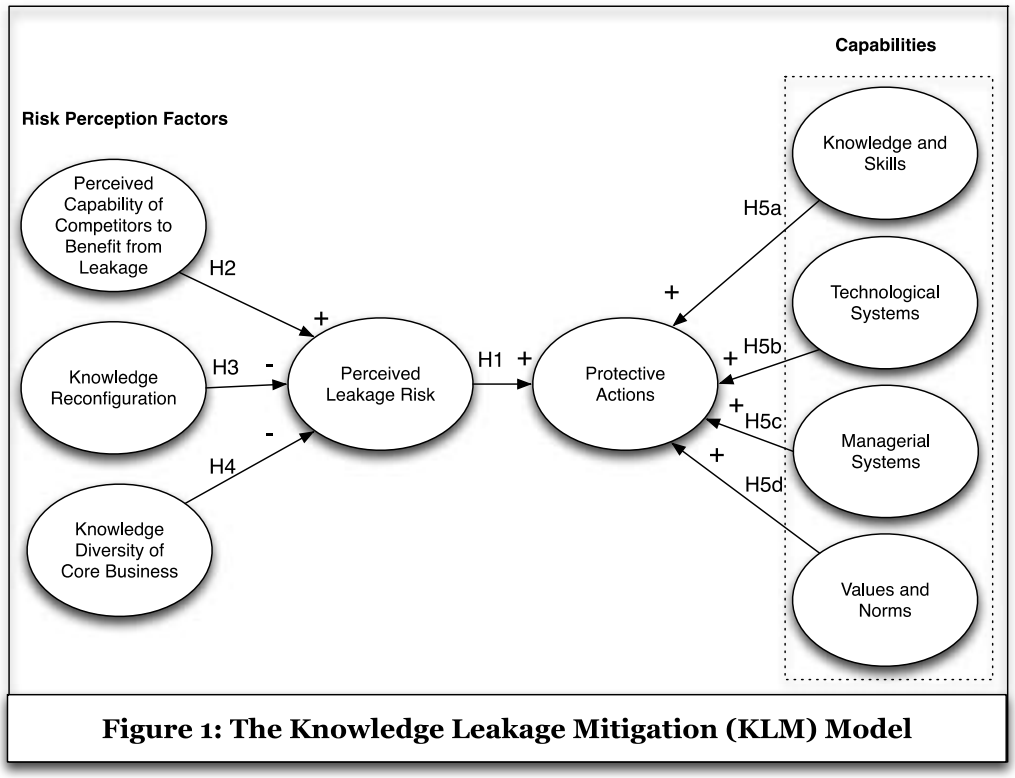

Figure 1: The Knowledge Leakage Mitigation (KLM) Model

Perceived leakage risk is related to Protective Actions

The KLM model is centered around the fundamental assertion of security risk theory, i.e., the relationship between an organization's perceived leakage risk and the resulting range of protective actions it develops in response.

Perceived risk of leakage is based on the classical definition of risk (AS/NZS ISO/IEC 27005:2011), and is defined as the combination of two factors: 1) the probability that sensitive knowledge will leak and 2) the impact of the leakage of sensitive knowledge on the organization.

Protective actions are enabled by leakage mitigation capabilities as discussed in the RBT-literature (e.g. Leonard-Barton 1992; Teece, 2009). Previous research has established that organizational-level actions are at the core of business strategy and competitive positioning (Chen et al. 1992; Mintzberg 1978; Porter 1980). These may be competitive actions or protective actions. Whereas competitive actions aim at defending or improving an organization's relative competitive position (Chen 1988; Smith et al. 1992), the purpose of protective actions is to protect organizational assets in the market (Teece 2009).

Protective actions include the following (see Ahmad et al., 2014a): the application of management methodologies to identify knowledge that requires protection (Aljafari and Sarnikar 2009; Norman 2001; O'Donoghue and Croasdell 2009), the implementation of policies and procedures to support and enforce compartmentalization of sensitive knowledge (Amiri 2007; DeSouza 2006; O'Donoghue and Croasdell 2009), and the application of legal provisions such as NDAs (Chai et al. 2011; De Faria and Sofka 2010; Olander et al. 2009), the development of an information security culture through education, training and awareness (Siponen 2000; Wilson and Hash 2003), and the use of technical tools to regulate access to sensitive knowledge, such as Firewalls and VPNs over networks and Role Based Access Controls,

passwords and other authentication mechanisms over systems (Fung 2004; Liu and Ormaner 2009; Whitman and Mattord 2011;). And finally, using disruption and disinformation tactics to prevent competitors from benefiting from knowledge leakage (Jelen 1991; Joint Publication 3-13.3). Previous research has shown that a high perceived risk of leakage does not necessarily mean a high level of protective actions; therefore we need to test this finding in a large study. We hypothesize that:

H1: The higher the perceived risk of leakage, the greater the protective actions to mitigate leakage.

Additional Factors that Influence Perceived Leakage Risk

Having identified the fundamental hypothesis (H1), we return to the unresolved issue raised by Ahmad et al. (2014a) and propose a new research question:

Why do some knowledge-intensive, highly competitive organizations seem to adopt a laissez-faire approach to knowledge leakage mitigation?

Based on our literature review, we suggest the following three additional factors may influence the perceived risk of leakage thereby explaining the protective behavior of organizations: 1) perceived capability of competitors, 2) knowledge reconfiguration, and 3) knowledge diversity of core business. These are explained below:

Factor 1: Perceived Capability of Competitors

We argue that an organization's perception of leakage risk is positively related to its perception of the capabilities of their competitors to benefit from the leakage. Therefore, we define this factor as the extent to which competitors are able to take advantage of knowledge leakage to increase their competitiveness (in this regard we draw on the intelligence literature e.g. Jelen 1991 and Joint Publication 3-13.3). Specifically, the capability of competitors may influence the organization' risk perception in two ways: First, a competitor with clear intent to challenge an organization's competitive advantage may take active steps to acquire sensitive knowledge to improve their competitiveness. This increases the perceived likelihood that knowledge may leak, e.g. through recruitment of knowledgeable personnel, online activities, monitoring of social media, etc. Second, the competitor may be perceived to have the ability to draw useful insights and inferences from even minimal leakage, thus ultimately increasing their own competitiveness. This elevates the impact of leakage if it were to occur. Therefore:

H2: The greater the perceived capability of competitors to benefit from leakage, the higher the perceived risk of leakage

Factor 2: Knowledge Reconfiguration

We also argue that the organization's perceived risk of leakage is reduced if it believes that it can rapidly develop new capabilities by reconfiguring its knowledge assets (to offset its risk exposure). An organization's ability to reconfigure its existing knowledge assets is defined as the capability to combine and integrate its existing knowledge assets into new forms or opportunities that yield new products, processes, services or market-related knowledge (Grant 1996). Reconfiguration of existing knowledge assets depends on the assimilation of new knowledge from the environment and the organization's ability to combine and integrate this knowledge with existing knowledge (Lane and Lubatkin 1998; Van den Bosch et al. 1999). As such, an organization that is able to reconfigure its knowledge (through ongoing innovation, recombination, etc.), might be less affected by some inevitable knowledge leakage. Therefore:

H3: The greater an organization's ability to reconfigure is existing knowledge assets, the lower its own perceived risk of leakage

Factor 3: Knowledge Diversity of Core Business

Further, we argue that the organization's perceived risk of leakage is related to its knowledge diversity. An organization's knowledge diversity can be defined as its investment in diverse and complementing employee skills and a breadth of product, process and market-related knowledge (Smith et al. 2005; Van den Bosch et al. 1999; Volberda 1996). A breadth of employee skills can increase creativity and innovation in organizations, and a focus on learning in organizations may increase individuals' expertise in complementary knowledge domains. This enables the organization to transform its existing products,

services and processes in the event of unexpected changes in the business environment (as a result of leakage), thereby offsetting the risk. We hence hypothesize that:

H4: The greater an organization's knowledge diversity, the lower its own perceived risk of leakage

Factors that Influence Protective Actions

Following from our discussion on RBT and dynamic capabilities, we argue that organizational actions taken to protect knowledge stem from leakage mitigation capability. Indeed, in cases where organizational knowledge is instrumental to its competitive advantage, we argue such a capability should be considered as part of its core capabilities (see Leonard-Barton 1992; Teece et al. 1997).

Therefore, for our KLM model, we adopt Leonard-Barton's (1992, p.113) capability framework based on four factors: 1) employee skills and knowledge, embedded in 2) technical systems, guided by 3) managerial systems, and underpinned by organizational 4) values and norms. We propose a leakage mitigation capability is a synergistic combination of these four factors. We argue that an organization will typically seek to mitigate its leakage risk through a capability that enables it to take protective actions in line with the level of perceived risk. Hence, for an elevated perceived level of risk, a more sophisticated protective capability might be expected (and vice versa). Hence, we hypothesize that:

H5a-5d: the sophistication of an organization's capability to take protective actions against leakage derives from a synergistic combination of employee skills and knowledge, technical systems, managerial systems, and values and norms.

Proposed Research Approach and Anticipated Contributions

In order to validate the Knowledge Leakage Mitigation model, we are designing a large-scale survey aimed at knowledge-intensive small, medium, and large organizations operating in a competitive environment. To accommodate for potential variation in the data, we will seek at least 1000 responses across a broad range of organizations in Australia. The research design targets organizations with competitive knowledge that is essential to their performance. The survey will include sectors such as banking, telecommunications, consulting, manufacturing, logistics, retail and utilities.

We have designed a draft survey instrument, which has been developed according to the ten steps embedded in the six scale development phases recommended by Mackenzie et al. (2011) i.e. conceptualization, development of measures, model specification, scale evaluation and refinement, validation, and norm development. Key constructs that relate to leakage with perceived leakage risk were conceptualized as the independent variables and protective actions as the dependent variable.

We have also identified a set of scales to measure each of the theoretical constructs in the research model. The measures were derived using a combination of literature analyses, and a qualitative study that we conducted prior to this research. Given the competitively sensitive nature of this research, we anticipate that some respondents might hesitate to comment on the exact nature of their knowledge mitigation approaches, etc. Therefore, we developed a number of representative scenarios for the survey where we ask respondents to make comparisons with their own organizational situation. We expect this approach will overcome some of the inherent sensitivities, especially in terms of perceived leakage risk identification.

The model and the survey instrument were tested and refined in two focus groups of seven and eight participants respectively: 1) knowledge managers responsible for strategy in their respective organizations and 2) information security consultants from leading management consulting organizations. Participants worked in a variety of industries or worked in consulting with different client industries. Each focus group lasted two hours. Participants in both focus groups were highly engaged with the KLM model leading to rich discussions on the concepts of leakage and risk.

Both stakeholder communities were invited to comment on each construct and associated hypotheses in the KLM model and to suggest other possible factors. In summary, both communities agreed that the KLM model constructs and relationships were conceptually sound. Focus group participants provided valuable feedback towards improving the survey scenarios and the terminology in the survey items to make the survey more accessible to industry. The refined survey will be deployed using an online survey

instrument. Survey data will be analyzed using covariance-based Structural Equation Modeling (SEM) (Byrne 2013). We plan to model the various theoretical constructs as latent variables with indicators as measures to test the hypotheses and implied relations between the constructs.

Anticipated Contributions

While there have been some prior studies into some aspects relating to knowledge leakage, our review of the literature suggests this will be one of the first large-scale empirical investigations into how organizations mitigate against leakage of competitive knowledge. We anticipate two contributions:

First, with reference to the findings in Ahmad et al. (2014a), we expect that the inclusion of additional constructs (knowledge diversity, knowledge reconfiguration, perceived capability of competitors) will provide a better explanation of how knowledge-intensive organizations perceive leakage risk (unresolved issue #3) and why they do not necessarily take extensive protective actions to secure their competitive knowledge (unresolved issue #4). Should this be confirmed empirically, that would mean these organizations are effectively hedging their knowledge leakage risk. Such organizations perceive their rivals do not have the necessary capability to benefit from eventual leaks, or if they do, that they would be able to reconfigure the knowledge, or rely on the diversity of their organizational knowledge in terms of competitive advantage. We will control for variation, e.g. the specific industry, the nature of the business, and the role/seniority of respondents to identify the spectrum of organizations, which perceive themselves to be exposed to knowledge leakage risk.

Second, we expect to be able to explicate what leakage mitigation capabilities look like and how they enable organizations to take protective actions (unresolved issues #1 and #2). Despite the wealth of literature on resources/capabilities, it remains nontrivial to measure the sophistication of complex organizational capabilities such as leakage mitigation in this study. As such, one of the potential methodological contributions from this study might be towards the measurement of complex organizational capabilities. Based on Leonard-Barton's (1992) capability dimensions, we postulate that the range of protective actions (i.e., what an organization can do to mitigate against leakage) derive synergistically from different capability dimensions (skills, technical systems, managerial systems, values and norms). This informs other studies that seek to assess complex capabilities.

Summary

In this paper, we have described a study into how organizations mitigate against perceived knowledge leakage in terms of developing a protective capability. We have proposed a Knowledge Leakage Mitigation model, which forms a theoretical basis for conducting a large-scale empirical survey of knowledge-intensive organizations in Australia. This research model synthesizes several related theoretical constructs, to better explain organizational approaches towards leakage mitigation, whilst factoring in their perceived risk. We anticipate this study will contribute towards a more informed understanding of the risk of organizational knowledge leakage, and the protective actions organizations should take in response.

References

Ahmad, A., Bosua, R., and Scheepers, R. 2014a. "Protecting Organisational Competitive Advantage: A Knowledge Leakage Perspective", Computers & Security (42), pp. 27-39.

Ahmad, A., Maynard, S. B., Park, S. 2014b. "Information Security Strategies: Towards an Organizational Multi-Strategy Perspective," Journal of Intelligent Manufacturing (25), pp. 357-370.

Aljafari, R. and Sarnikar, S. 2009. "A Framework for Assessing Knowledge Sharing Risks in Interorganizational Networks," AMCIS 2009.

Amiri, A. 2007. "Dare to Share: Protecting Sensitive Knowledge with Data Sanitization," Decision Support Systems (43), pp. 181-191.

AS/NZS ISO/IEC 27005:2011 (2011). Information technology - Security techniques - Information security risk management (ISO/IEC 27005:2011, MOD).

Athanasopoulos, E., Makridakis, A., Antonatos, S., Ioannidis, S., Anagnostakis, K., Markatos, E. 2008. "Antisocial Networks: Turning a Social Network into a Botnet", 11th Information Security Conference.

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage," Journal of Management (17), pp. 99-120.

Barney, J. 1996. "The Resource-based Theory of the Firm". Organization Science (7), pp. 469-479.

Barney, J., and Hesterly, W. S. 2006. Strategic Management and Competitive advantage: Concepts and Cases, Boston:Prentice-Hall.

BioSpectrum (2013): http://www.biospectrumasia.com/biospectrum/news/197883/eli-lilly-scientists-accused-leaking-trade-secrets#.U2Maal5V9H0

Blasco, A., and Jorge, X. 2013. "Bypassing information leakage protection with trusted applications," Computers and Security (31:4), pp. 557-568.

Boisot, M., and Canals, A. 2004. "Data, information and knowledge: have we got it right?," Journal of Evolutionary Economics (14:1), pp. 43-67.

Brown, J.S., Duguid, P. 2001. "Structure and Spontaneity: Knowledge and Organization," in I. Nonaka and D.J. Teece, (eds.), Managing Industrial Knowledge, Creation, Transfer and Utilization. London: SAGE publications.

BusinessWeek (2011): http://www.businessweek.com/news/2011-09-15/kolon-loses-920-million-verdict-to-dupont-in-trial-over-kevlar.html

Byrne, B. M. 2013. Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming. Routledge.

Carvalho, V. R., Balasubramanyan, R., and Cohen, W. W. 2009. "Email Leaks and Recipient Suggestions: A User Study with Mozilla Thunderbird," CHI 2009.

Chai, K. H., Yap, C. M., and Wang, X. 2011. "Network Closure's Impact on Firms' Competitive Advantage: The Mediating Roles of Knowledge Processes," Journal of Engineering and Technology Management (28:1), pp. 2-22.

Chen, M. J., Smith, K. D., and Grimm, C. M. 1992. "Action Characteristics as Predictors of Competitive Responses," Management Science (38), pp. 439-455.

CISCO. 2008. "Data leakage worldwide: common risks and mistakes employees make," CA9 2008.

Colwill, C. 2009. "Human Factors in Information Security: The Insider Threat - Who Can You Trust These Days"? Information Security Technical Report (14), pp. 186-196.

Dahlbom, B. and Mathiassen, L. 1993. Computers in context: The philosophy and practice of systems design. Blackwell Publishers Inc.

Davenport, T. and Prusak, L. 1998. Working Knowledge: How Organizations Manage What They Know. Boston:Harvard Business School Press.

De Faria, P. and Sofka, W. 2010. "Knowledge Protection Strategies of Multinational Firms - A Cross-Country Comparison," Research Policy (39:7), pp. 956-968.

DeSouza, K. C. 2006. "Knowledge Security: An Interesting Research Space," Journal of Information Science and Technology (25), pp. 85-98.

Dhillon, G. 2006. Principles of Information Systems Security. John Wiley and Sons.

Earl, M. 2001. "Knowledge Management Strategies: Towards a Taxonomy," Journal of Management Information Systems (18), pp. 215-233.

Easterby-Smith, M., Lyles, M. A., and Tsang, E. W. K. 2008. "Inter-Organizational Knowledge Transfer: Current Themes and Future Prospects," Journal of Management Studies (45), pp. 677-690.

Fung, K.T. 2001. Networking Security Technologies, CRC Press.

Furnell, S., and Botha, R. A. 2011. "Social Networks - Access All Areas?" Computer Fraud and Security (5), pp. 14-19.

Gold, A. H., Malhotra, A., Segars, A. H. 2001. "Knowledge Management: An Organizational Capabilities Perspective," Journal of Management Information Systems (18), pp. 185-214.

Grant, R. M. 1996. "Toward a Knowledge-Based Theory of the Firm," Strategic Management Journal (17), pp. 109-122.

Grant, R. M. 1997. "The Knowledge-Based View of the Firm: Implications for Management Practice," Long Range Planning (30), pp. 450-454.

Gross, R. and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks (The Facebook Case)," ACM Workshop on Privacy in the Electronic Society (WPES).

Hansen, M., Nohria, N., and Tierney, T. 1999. "What's Your Strategy for Managing Knowledge?" Harvard Business Review (77), pp. 106-116.

Hildreth, P. M., Kimble, C. 2002. "The Duality of Knowledge," Information Research (8:1).

Holsapple, C., Jones, K. 2005. "Exploring Secondary Activities of the Knowledge Chain," Knowledge and Process Management (12), pp. 3-31.

Huth, C. L. 2013. "Guest editorial: A brief overview of data leakage and insider threats," Information Systems Frontiers, pp. 1-4.

Jagatic, T., Johnson, N., Jakobsson, M., Menczer, F. 2007. "Social Phishing," Communications of the ACM (20), pp. 94-100.

Jansen, J. 2010. "Strategic Information Disclosure and Competition for an Imperfectly Protected Innovation," The Journal of Industrial Economics (58), pp. 349-372.

Jelen, G. F. 1991. "The Defensive Disciplines of Intelligence," The International Journal of Intelligence and Counterintelligence (5), pp. 381-399.

Joint Publication 3-13.3: Operations Security." Joint Staff, n.d.

Jones, A., Ashenden, D. 2005. Risk Management for Computer Security. Elsevier Butterworth-Heinemann, Oxford.

Lane, P. J. and Lubatkin, M. 1998. "Relative Absorptive Capacity and Interorganizational Learning," Strategic Management Journal (19:5), pp. 461-477.

Lavie, D. 2006. "The Competitive Advantage of Interconnected Firms: An Extension of the Resource-Based View," Academy of Management Review (31:3), pp. 638-658.

Leonard-Barton, D. 1992. "Core Capabilities and Core Rigidities: A Paradox in Managing New Product Development," Strategic Management Journal (13), pp. 111-126.

Liu, S. and Ormaner, J. 2009. "From Ancient Fortress to Modern Cyberdefense," IT Professional (11).

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. "Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques," MIS Quarterly (35:2), pp. 293-334.

Mahoney, J. T. and Pandian, J. R. 1992. "The Resource-Based View Within the Conversation of Strategic Management," Strategic Management Journal (13), pp. 363-380.

Marabelli, M. and Newell, S. 2012. "Knowledge Risks in Organizational Networks: The Practice Perspective," Journal of Strategic Information Systems (21), pp. 18-30.

Michal, K. 1994. "Business Counterintelligence and the Role of the U.S. Intelligence Community," International Journal of Intelligence and CounterIntelligence (7:4), pp. 413-427.

Mintzberg, H. 1978. “Patterns in Strategy Formation,” Management Science (24), pp. 934-948.

Nonaka, I. 1994. "A Dynamic Theory of Organizational Knowledge Creation," Organization Science (5), pp. 14-37.

Nonaka, I., Toyama, R., and Konno, N. 2000. "SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation," Long Range Planning (33), pp. 5-34.

Norman, P.M. 2001. "Are Your Secrets Safe? Knowledge Protection in Strategic Alliances," Business Horizons (Nov-Dec), pp. 51-60.

O'Donoghue, N. and Croasdell, D. T. 2009. "Protecting Knowledge Assets in Multinational Enterprises: A Comparative Case Approach," VINE (39), pp. 298-318.

Olander, H., Hurmelinna-Laukunnen, P., and Mahonen, J. 2009. "What's Small Size Got to do With it? Protection of Intellectual Assets in SMEs," International Journal of Innovation Management (13), pp. 349-370.

Penrose, E. T. 1959. The Theory of the Growth of the Firm. Cambridge, MA.

Polanyi, M. 1966. The Tacit Dimension, New York:Doubleday & Company Inc.

Porter, M. E. 1980. Competitive Strategy, New York:Free Press.

Ristenpart, T., Tromer, E., Shacham, H., Savage, S. 2009. "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Computer Clouds," The Conference on Computer and Communications Security, Illinois, USA.

Shedden, P., Smith, W., Ahmad, A. 2010. "Information Security Risk Assessment: Towards a Business Practice Perspective," in Proceedings of the 8th Information Security Management Conference, Perth, Australia: Edith Cowan University, pp. 127-138.

Shedden, P., Scheepers, R., Smith, W., and Ahmad, A. 2011. "Incorporating a Knowledge Perspective into Security Risk Assessment," VINE: Journal of Knowledge Management (41), pp. 152-166.

Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," Information Management and Computer Security (8:1), pp. 31-41.

Smith, K. G., Collins, C. J., and Clark, K. D. 2005. "Existing Knowledge, Knowledge Creation Capability, and the Rate of New Product Introduction in High-Technology Firms," Academy of Management Journal (48:2), pp. 346-357

Straub, D., Rai, A., and Klein, R. 2004. "Measuring Firm Performance at the Network level: A Nomology of the Business Impact of Digital Supply Networks," Journal of Management Information Systems (21), pp. 83-114.

Szulanski, G. 2000. "The Process of Knoweldge Transfer: a Diachronic Analysis of Stickiness," Organizational Behaviour and Human Decision Processes (82), pp. 9-27.

Tan, J., Bosua, R., Ahmad, A. 2010. Reconciling the Availability and Confidentiality of Knowledge Assets in Organizations, Unpublished Honours dissertation. The University of Melbourne, Melbourne, Australia.

Teece, D. J. 2007. "Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance," Strategic Management Journal (28:13), pp. 1319-1350.

Teece, D. J. 2009. Dynamic Capabilities and Strategic Management. Oxford:Oxford University Press.

Trkman, P., Desouza, K. 2012. "Knowledge Risks in Organizational Networks: An Exploratory Framework," Journal of Strategic Information Systems (21), pp. 1-17.

Van den Bosch F. A. J., Volberda, H. W. and de Boer, M. 1999. "Coevolution of firm absorptive capacity and knowledge environment: Organizational forms and combinative capabilities," Organization Science (10), pp. 551–568.

Volberda, H. W. 1996. "Toward the Flexible Firm: How to Remain Vital in Hypercompetitive Environments," Organization Science (7:4), pp. 359–387.

Von Solms, B. 2006. "Information Security - The Fourth Wave," Computers & Security (25:3), pp. 165-168.

Wernerfelt, B. 1984. "A Resource-Based View of the Firm," Strategic Management Journal (5:2), pp. 171-180.

Whitman, M. E., Mattord, H. J. 2011. Principles of Information Security, 4th edition, Boston: Thomson Course Technology.

Wilson, M. and Hash, J. 2003. "Building an Information Technology Security Awareness and Training Program." NIST Special publication 800:50.